IN THE SPECIFICATION

Please replace the paragraph beginning on page 3, line 13 with the following paragraph:

a1 In order to overcome the above limitations of the prior art, it is an aspect of the invention to provide a method of ciphering data received by a gateway, the data ciphered absent accessing the memory buffer via the data bus.

Please replace the paragraph beginning on page 3, line 16 with the following paragraph:

a2 It is an aspect of the invention to provide a method of encoding data for transmission via a wide area network, the data ciphered and processed for determining integrity in parallel.

Please replace the paragraphs beginning on page 3, line 20 and page 3, line 26 with the following paragraphs:

a3 In a first aspect, a system for ciphering data for transmission by a communication device is provided. The system includes a memory device having a memory buffer a first access port connected to the memory buffer and a second access port connected to the memory buffer. The system also has a data processing processor connected to the first access port via a first bus and a ciphering processor connected to the second access port via a second bus. The first access port and the second access port each provide mutually independent access to the memory buffer. The second bus is not connected to the first bus. The data processing processor is adapted to receive the data and provide the data to the memory buffer over the first bus. The ciphering processor is adapted to retrieve the data from the memory buffer over the second bus, generate ciphered data from the data, generate integrity check information for the ciphered data using the data and provide the ciphered data to the memory buffer over the second bus.

The ciphering processor may include an encryption module for generating the ciphered data and a hashing module for generating the integrity check information.

The ciphering processor may include an encryption module for generating the ciphered data and a message digesting module for generating the integrity check information.

The encryption module may include a DES encryption module for performing one of DES and triple-DES encryption.

The hashing module may include a HMAC hashing module for encoding the integrity check information within the ciphered data.

The memory buffer may include dual port random access memory.

The data processing processor may include a security module. The security module may retrieve a security context from memory. The security context may be used in generating the ciphered data.

The security module may determine a security context relating a source of the data or a destination for the ciphered data and may store the security context in the memory buffer. The security context stored may be accessible by the ciphering processor.

The data processing processor may include a security address module. The security address module may store an address associated with the security context in the memory buffer. The address may be based on the source of the data or the destination for the ciphered data.

The security module may provide an indication to the data processing processor when a security context is not present in the memory buffer.

The data processing processor may operate asynchronously to the ciphering processor.

The data processing processor may be clocked by a first clock source and the ciphering processor may be clocked by a second clock source. The first clock source may be asynchronous to the second clock source.

The system may further include a first communications port at which the data is received and a second communications port over which the data processing processor transmits the ciphered data.

The data received at the first communications port may include fragments of a packet. The data processing processor may store the fragments in the memory buffer to assemble the packet. The ciphering processor may generate the ciphered data from the assembled packet.

The system may be disposed at a gateway between a private network and a public network in a secure virtual private network. The first communications port may be connected to the private network or the public network and the second communications port may be connected to the other one of the private network and the public network.

Please replace the paragraph beginning on page 4, line 26 with the following paragraph:

When the beginning of a packet is detected by the processor 7, a new file within the memory is created or a new portion of the memory is allocated for the packet. A ciphering circuit 8 then retrieves the file from the memory buffer 3 via the data bus 2. The data within the buffer memory 3 is ciphered and data integrity information is generated for data integrity verification. The ciphered data is then stored in the buffer memory 3 via the data bus 2. When data is being secured for transmission via a wide area network, the integrity information is stored

a4 with the ciphered information. The processor 7 then retrieves the ciphered information from the buffer memory 3 via the data bus 2 and provides it to the second communication port 4b.

Please replace the paragraph beginning on page 5, line 18 with the following paragraph:

When the beginning of a packet is detected by the processor 7, a new file within the buffer memory 5 is created. A ciphering processor 13 then retrieves the file from the buffer memory 5 via a second other data bus. The data within the buffer memory 5 is ciphered and data integrity information is generated for data integrity verification. The ciphered data is then stored. When data is being secured for transmission via a wide area network, the integrity information is stored with the ciphered information. The processor 7 then retrieves the ciphered information and provides it to the second communication port 4b.

a5

Please replace the paragraph beginning on page 5, line 25 with the following paragraph:

Clearly, processing of a packet requires at least two data bus operations, half of the prior art implementation. Thus, using a system as described herein, performance is improved substantially. Also, since the ciphering processor 13 operates independent of the processor 7 and of the data bus 2, it is possible to clock the ciphering processor 13 independent of the other processor 7. Therefore, when ciphering operations prove to be a bottleneck, a faster ciphering processor 13 is used. Alternatively, when the processor 7 is the bottleneck, a faster processor 7 is used.

a6

Please replace the paragraph beginning on page 6, line 3 with the following paragraph:

The buffer memory 5 is preferably formed of dual ported random access memory. Of course, when reduced performance is acceptable, a random access memory arbitration circuit (not shown) is used to arbitrate access to the random access memory making it function similarly to dual ported memory. In essence, either the ciphering processor 13 or the processor 7 are switched to drive the memory circuitry. By using true dual ported random access memory, both the processor 7 and the ciphering processor 13 can access the buffer memory 5 simultaneously. This effectively eliminates operations of one processor from affecting operation the other.

a7

Please replace the paragraph beginning on page 6, line 11 with the following paragraph:

At least four memory access operations are required to process a packet; however, they are now performed two on the data bus 2 and two on a second other data bus. This is highly advantageous as described above.

a8

Please replace the paragraph beginning on page 6, line 14 with the following paragraph:

The implementation of ciphering and data integrity operations in parallel improves system performance. Prior art systems perform one operation and then the other. Implementation of the two operations in parallel requires some set up operations and a final operation of the data integrity processing. That said, it reduces two sequential operations to one operation equal to the greater of the two. The improved efficiency allows for a ciphering processor 13 having reduced performance and yet capable of achieving a same overall data throughput.

a9

Please replace the paragraph beginning on page 7, line 13 with the following paragraph:

Thus, it is clear that implementation of these functions in parallel within a single ciphering processor is advantageous. Further, since the processed data is the same data in both functions, the use of a single integrated processor reduces memory access operations since the same data is used by each of the processing portions of the ciphering processor 13. This has an added advantage of increasing performance through reduced access to external memory.

Please replace the paragraph beginning on page 7, line 18 with the following paragraph:

When a packet is ciphered according to the invention and results in a packet that is too large for transmission via a network, the packet is fragmented. Such a packet has two fragments. In this case, the receiving end may be optimized to process paired fragments.

Please replace the paragraph beginning on page 8, line 21 with the following paragraph:

The ciphering system in the form of an ASIC or an FPGA includes means to look up the security association determined by the host processor. The security association is, for example, the context in which a packet is to be ciphered including keys and ciphering algorithms. The host processor includes means for determining a security association and for storing the determined security association in a location accessible by the ciphering processor. For example, the security association is stored in the dual ported RAM. Alternatively, the security association is stored in memory within the ciphering processor.